

Enhancing Cybersecurity through Effective penetration testing and Vulnerability Scanning

www.doi.org/10.62341/nakt1429

Ahmed Elstia, Khelifa Masoud, Nowh Saad, Talal Gigma

Higher Institute of science and Technology Tamzawa Ashati, Libya
Department of computer technology, Department of Electronic and
Electrical Technology
aelstia@gmail.com

Abstract

The number of computer network attacks today is increasing with the sophisticated attack tools and complicated methods hence, building secure systems is required. The demand for regular penetration testing and vulnerability scanning has become an urgent issue. This paper focuses on increase the security of the system resources being tested; Determine the weakness in the popular operating systems; Focus on methodologies and approaches to analyze the system for security that leads to protect the system against external threats. An experimental setup of a virtual penetration testing environment lab is created on a system using virtualization software. By using of the most powerful tools and techniques used today, a successful penetration testing and vulnerability scanning through three phases of processes are implemented. Eventually, the results of this process will help identify potential vulnerabilities in the operating systems and ways to patch them up.

Keywords: Cybersecurity, penetration testing, vulnerability scanning tools.

تعزيز الامن السيبراني من خلال اختبار الاختراق الفعال وفحص الثغرات

أحمد السطيل، خليفة مسعود، نوح رجب، طلال قيقمة

المعهد العالي للعلوم والتقنية تامزوة الشاطئ
قسم تقنيات الحاسوب، قسم التقنيات الكهربائية والالكترونية
aelstia@gmail.com

الملخص

يتزايد عدد الهجمات على شبكات الحاسوب اليوم مع استخدام أدوات هجوم متطورة، وأساليب معقدة ومن ثم فإن بناء أنظمة آمنة أمر مطلوب. أصبح الطلب على اختبارات الاختراق بشكل منتظم وفحص الثغرات الأمنية ضرورة ملحة. تركز هذه الدراسة الموارد على زيادة أمن النظام الذي يجري اختباره؛ تحديد نقاط الضعف في أنظمة التشغيل الشائعة؛ التركيز على منهجيات وأساليب تحليل النظام من حيث الأمان الذي يؤدي إلى حماية النظام من التهديدات الخارجية. تم إنشاء مختبر تجريبي لبيئة اختبار الاختراق افتراضية على نظام يستخدم برنامج محاكاة افتراضي. ومع استخدام أقوى الأدوات والتقنيات المستخدمة اليوم، حيث تم تنفيذ اختبار اختراق ناجح وفحص نقاط الضعف من خلال ثلاث مراحل من العمليات. وفي النهاية ستساعد نتائج هذه الدراسة في تحديد نقاط الضعف المحتملة في أنظمة التشغيل وطرق تصحيحها.

الكلمات المفتاحية: الأمن السيبراني، اختبار الاختراق، أدوات فحص الثغرات

1. Introduction

Vulnerability can come as a fault, weak point or even an error in the system that can be broken by an attacker who targets to change the ordinary behavior of the system. Number of vulnerabilities increases with increasing number of software systems. Additionally, as most of the systems are exposed to multiple users and to the internet, it is just a matter of time before someone can make an attack that results in unpredicted damages and cost. Generally, the goal of an attacker is to gain some privileges in the system to take

control of it or to achieve valuable information for his own benefit. Then it is crucial for the developers as well as users to be aware of vulnerabilities and their detection and prevention [1].

Plenty of Reports released that cyber-security attacks are becoming ever more complicated; however, many hackers still rely on decades-old tools and techniques such as phishing and hacking, and the attacks use a combination of these techniques and includes a secondary victim, adding sophistication to their breach.

Another troubling issue is that lots of existing vulnerabilities stay open, mostly because security patches that have long been available have never been implemented. Indeed, most of the vulnerabilities arise from a breach that exists since 2007.

More importantly, new vulnerabilities come up daily because of software errors, poor configuration of applications, and human errors. When exposed, these vulnerabilities can result in unpredicted program behavior, illegal network access, privacy violations, and broken up business operations. Once the data is classified as critical, automating the analysis of the vulnerabilities will allocate remediation efforts to focus on critical risks rather than time-consuming low-risk assets [2].

2. Penetration testing vs Vulnerability scanning

2.1 Penetration Testing:

Penetration testing, also known as ethical hacking or pen testing, is a security assessment technique where skilled professionals simulate real-world attacks to identify vulnerabilities in a system or network. The main objectives of penetration testing are: Detecting vulnerabilities, Evaluating impact, and providing actionable insights. In summary, penetration testing step by step procedure to deal with found weaknesses and evaluate their impact, providing organizations with actionable insights to improve their security attitude [3].

2.2 Vulnerability Scanning:

Vulnerability scanning, on the other hand, is a systematic process of identifying and quantifying vulnerabilities within a system or network. It involves using automated tools and techniques to scan

systems for known vulnerabilities. The main objectives of vulnerability assessment are: Identifying vulnerabilities, and quantifying risk. Vulnerability assessments are generally less invasive and usually focus on identifying known vulnerabilities. They provide organizations with insights into the security weaknesses present in their systems, enabling them to take appropriate actions to remediate those vulnerabilities [3][4].

3. System scanning

System scanning is a procedure for identifying active hosts on a system, either with attacking purposes or for system security assessment. Scanning systems, for example, ping breadths and port scans, return information about which IP addresses map to live hosts that are active on the Internet and what administrations they offer. Another inspection strategy, converse mapping, returns data about what IP addresses don't map to live hosts. This method empowers an attacker to make suspicions about practical locations.

Scanning is one of three parts of knowledge social event for an attacker. In the foot printing stage, the attacker makes a profile of the target system, with data, domain name system (DNS), e-mail servers and IP address range. Most of this information is available online. In the checking stage, the attacker collects data about the particular IP addresses that can be reached over the Internet, their operating systems, system architecture, and the services running on each computer. In the enumeration stage, the attacker accumulates data; gather client names and id's, routing tables, and Simple Network Management Protocol (SNMP) information [5].

4. Host scan and OS fingerprinting

Refer to efforts to find out about computer systems and their networks, or footprints. Even though foot printing should be possible for true legitimate purposes, the term is regularly connected to hacking and cyber-attacks.

Regarding hacking, the term foot printing is given to some portion of the work that hackers do unobtrusively, behind the scenes, before they attack a system. This may include taking a gander at what operating system an equipment setup uses or pinging the system to

decide major properties. Port scanning or registry questions are other types of foot printing. This type of data is used to plan for a cyber-attack. In that sense, the word foot printing is utilized as a part of data innovation like the word packaging is utilized for house robbery.

Regardless of its sometimes-wicked notion; public tools exist for footprinting, including open-source tools for Windows and Linux. These types of tools can help to peek into URL handling, SSL certificates and other legitimate parts of system security. These can be used to simply monitor a system or to look for its weaknesses in terms of network security [6].

5. Port scan

Port scanning identifies which ports are accessible (i.e., turned on by an administration). Since open ports may infer security weaknesses; port checking is one of the essential discovery methods used by attackers. In this manner, security scanning should dependably incorporate port scanning. Be that as it may, some defenselessness scanners have a pre-characterized default.

The demonstration of systematically scanning a PC's ports since a port is a gateway where data goes into and out of a PC, port scanning discovers open doors into a PC. Besides authorized usage to test systems for vulnerabilities, port scanning can also be perniciously used by unauthorized parties that want to break into that PC.

A port output is a progression of messages each related with a well-known port number that the computer provides. These messages are sent by somebody endeavouring to break into a PC to detect which PC is responsible for administration. Port scanning, a favorite approach of a computer cracker, gives the attacker an idea about where to test for weaknesses. Basically, a port sweep comprises of making an impression on each port one by one. The type of received response shows whether the port is in use and can be tested for weakness.

Many tools and techniques have been proposed to help ease the difficulty in discovering vulnerability. Not all techniques and the

tools are the same, so the developers are left to decide how they can best discover vulnerabilities on their own.

For general network monitoring and analysis, there are various tools utilizing The Internet Control Message Protocol (ICMP) and the Simple Network Management Protocol (SNMP), such as Nmap and Metasploit [6].

Nmap is a network mapping and information gathering tool, further classified as sniffing and mapping device. Sniffing devices are utilized to catch, take a snapshot, and examine organized traffics. Then again, mapping tools are utilized to detect an active host on a system. These tools provide a complete status report concerning network hosts, ports, etc. Similarly, another tool utilized for both hacking and shielding, Metasploit Framework is a device for creating and executing abuse code against a remote target machine. Actually, data gathering devices are utilized by both safeguards and aggressors. Before launching an attack, intruders need to know the properties of the network, such as ideal nodes to launch attacks. Therefore, intruders first collect information about networks, such as IP addresses and operating systems to find vulnerable spots in such networks using different information gathering tools. After gathering enough information, intruders apply their attacks to the networks [6].

6. System process phases

6.1 Reconnaissance (Information Gathering) Phase

This step comes before any real attacks are planned. The idea is to gather as much data as possible to serve the purpose, like IP packets to figure out what hosts are accessible on the system, what administrations (application name and version) those hosts are putting forth, what working frameworks (and OS variants) they are running, what sort of packet channels/firewalls are being used. To achieve this, we will use a specific tool and gather relevant information [6]. Figure 1 shows Reconnaissance phase.

6.2 Weakness Discovery Phase:

The information collected during the reconnaissance phase is an input to this phase in which network scanning and detecting

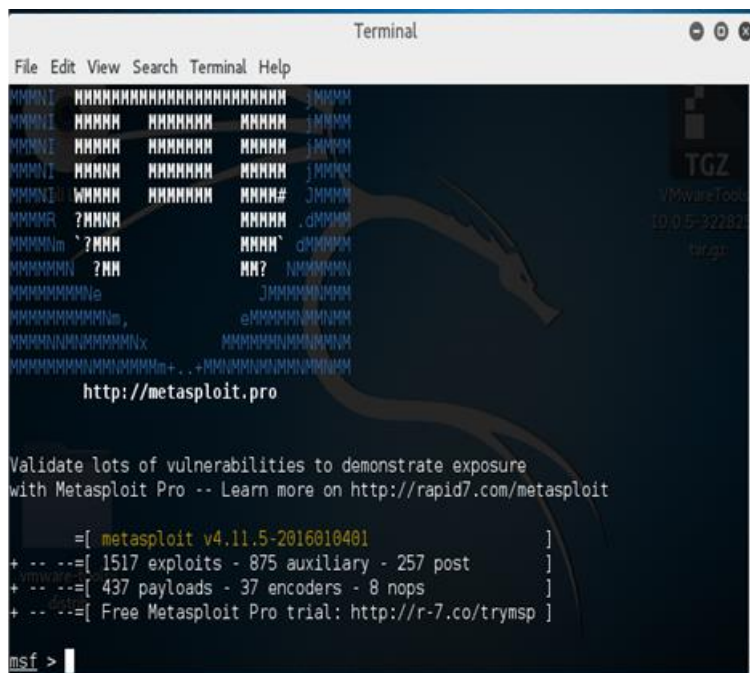
potential vulnerabilities within the system are performed. The goal is to discover vulnerabilities in the network systems, operating systems, servers, applications, and valuable data before a hacker does [7].

```
root@kaliAHMED: ~  
File Edit View Search Terminal Help  
root@kaliAHMED:~# nmap -A 192.168.65.134  
Starting Nmap 7.01 ( https://nmap.org ) at 2016-04-12 23:50 EEST  
Nmap scan report for 192.168.65.134  
Host is up (0.00082s latency).  
Not shown: 996 closed ports  
PORT      STATE SERVICE        VERSION  
135/tcp   open  msrpc          Microsoft Windows RPC  
139/tcp   open  netbios-ssn   Microsoft Windows 98 netbios-ssn  
445/tcp   open  microsoft-ds  (primary domain: HOME)  
1025/tcp  open  msrpc          Microsoft Windows RPC  
1 service unrecognized despite returning data. If you know the service/version,  
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n  
ew-service :  
SF-Port445-TCP:V=7.01%I=7%D=4/12%Time=570D5FA9%P=1586-pc-linux-gnu%r(SMBPr  
SF:ogNeg,69,"\\0\0e\xffSMBr\0\0\0\0x88\01@\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0  
SF:\x06\0\0\01\0\0x11\07\0\0x03\0\0\01\0\04\01\0\0\0\0\01\0\0\0\0\0\0xf  
SF:d\xe3\01\0\0xa0\0c4\08a\0fb\0xc\094\0d1\001L\xff\00\0x20\0\0\0fc\xe3\15\  
SF:xb1ly\x80iH\00\0E\0\0W\0I\0N\0X\0P\x062\0\0\0");  
MAC Address: 00:0C:29:7A:4B:A5 (VMware)  
Device type: general purpose  
Running: Microsoft Windows 2003  
OS CPE: cpe:/o:microsoft:windows_server_2003::spl cpe:/o:microsoft:windows_ser  
r_2003::sp2
```

Fig.1. a part of Reconnaissance phase

6.3 Action Preparation Phase

This step uses the results of the discovery phase and describes the technical background of the security vulnerability and how it may be exploited. Moreover, a hazard investigation demonstrates potential hazards of possible defects in the general settings of the tested system. Finally, constructive solution proposals are given in the respective problem, to directly provide ideas for improvement and take proactive actions based on practical approaches [8]. One of tool was considered as an action and preparation tool is Metasploit framework, it was conducted for discovering and exploiting known vulnerability. Figure 2 shows Metasploit console.



```
Terminal
File Edit View Search Terminal Help
MMMMI  #####  #####  #####  #####
MMMMI  #####  #####  #####  #####
MMMMI  #####  #####  #####  #####
MMMMI  #####  #####  #####  #####
MMMMI  #####  #####  #####  #####
MMMMR  ?####  #####  #####  #####
MMMMm  `?###  #####  #####  #####
MMMMmM  ?##  ##?  #####
MMMMMMMMe  #####
MMMMMMMMMMm,  #####
MMMMMMMMMMMMMMx  #####
MMMMMMMMMMMMMMMMm+.  #####
http://metasploit.pro

Validate lots of vulnerabilities to demonstrate exposure
with Metasploit Pro -- Learn more on http://rapid7.com/metasploit

=[ metasploit v4.11.5-2016010401 ]
+ -- ==[ 1517 exploits - 875 auxiliary - 257 post ]
+ -- ==[ 437 payloads - 37 encoders - 8 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Fig.2. Metasploit console phase

7. Vulnerability Scanning and penetration testing Tools.

Let's say that all the operating systems and applications suffer from security flaws which appear from time to time and all developer companies trying to repair their products in order not to be exploited by hackers to harm the users.

The other thing that the cyber-attack report based on statistics and research documents Foundation the National Vulnerability Database of, which gathers data about vulnerability in systems and applications and it's considered as a huge database of such information, that each year there are an increase of the number of vulnerability discovered by the security researchers in both operating systems such as Android, Apple, Microsoft systems and Linux, Of course, 38 % of the security vulnerability are found in operating systems as indicated by National Vulnerability Database [9].

The information collected during the information gathering is used and exploit security weaknesses and performing system scanning and detecting potential vulnerabilities inside the system. Normally discovering vulnerabilities in the operating systems and identify the weaknesses and gen technical solution providing by scanning tool report and patch the vulnerability before a hacker detects [10].

A vulnerability scanner is a software package that executes the analytic phase of analysis, also identified as vulnerability assessment. Vulnerability investigation characterizes, distinguishes, and groups the security vulnerabilities in operating systems. Also, defenselessness investigation can assess the adequacy of the system. The acquired data in this phase for each scanning tool will be subject to statistics analysis to show the functionality of the tools, and the ability to discover more critical weaknesses with less false positive vulnerability numbers to determine the most effective one between the selected tools to perform the successful penetration testing.

8. Discussion

The main goal is to enhance the security and investigate the most powerful vulnerability scanning tools through the experimental methodology applied to virtual machine and analysis of the result of each scanning tools.

With the large number of penetration testing and vulnerability scanning tools, and for every phase of penetration testing there are many tools can be conducted to achieve a specific task, to determine which tool can be applied and identify a suitable penetration testing methodology, and which one is proper and useful to the tester to save time in an appropriate manner.

The experimental test is a virtual machine to simulate a virtual environment for penetration testing machine (attacker) and target machine (victims). For attacker machine Kali Linux distribution and windows 7 are used, (Nessus, OpenVAS, Nexpose, Retina) vulnerability tools scanning which compatible with Kali Linux and mostly are popular and free open-source tools. For target machine we used:

Windows XP pro, Windows 7, Windows 8.1, windows 10 pro, Linux Mint, Ubuntu, Windows Server 2012, and Ubuntu Server as a target machine to provide a wide knowledge and extend knowledge base of the users.

As can be clearly seen from the figures 3 that there is differentiation from the number of detected vulnerabilities by vulnerability scanning tools, where Nessus tool was detected the highest number of vulnerabilities, followed by OpenVAS, then Retina, and the come Nexpose.

But if the number of severity vulnerability considered (Critical, High, Medium, Low), the Nexpose tool detected the highest number of 25 vulnerability were detected 5 vulnerabilities as critical, 8 vulnerabilities labelled as high, 12 vulnerability classified as medium severity. Followed by Nessus and OpenVAS, each of the detected 12 vulnerability, Nessus detected 4 as critical, 1 as high, and 7 as a medium severity and low vulnerability detected by Nessus. OpenVAS detected 2 as high, 6 as medium, and 4 as a low severity, while no critical vulnerability discovered by OpenVAS. By discovering severity of vulnerability which can be exploitable figures 4,5,6,7 show the classification of OSs vulnerability detected by (Nessus, OpenVAS, Retina, Nexpose) tools respectively, and what's the procedures should be taken to harden the system and mitigate the effect of this vulnerability, especially the vendors of software still not patch the vulnerability yet. From the database of vulnerability, such as NVD (National Vulnerability Database), CVE (Common Vulnerability and Exposures), (NVT) Network Vulnerability Tests since the selected vulnerability scanning tool in this procedure depends on these databases to detect the vulnerability. In addition, practical recommendations to mitigate or remediate such security weaknesses are provided from the result of effective scanning tool.

In the third place comes Retina by 5 vulnerabilities, 4 of them are classified as a critical, and 1 vulnerability as a low severity, while no high or medium severity vulnerability discovered by Retina tool. The result demonstrates the most powerful tool used today between

the selected ones we considered the tool which can discover the critical and high severity vulnerability.

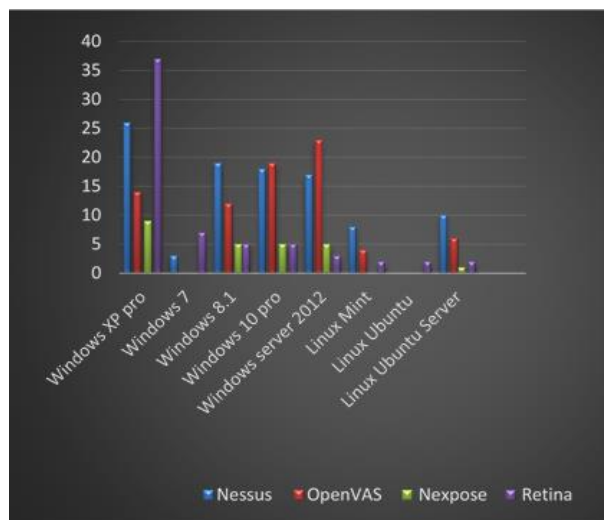


Figure 3. The Number of OSs Vulnerability Detected by Scanning Tools

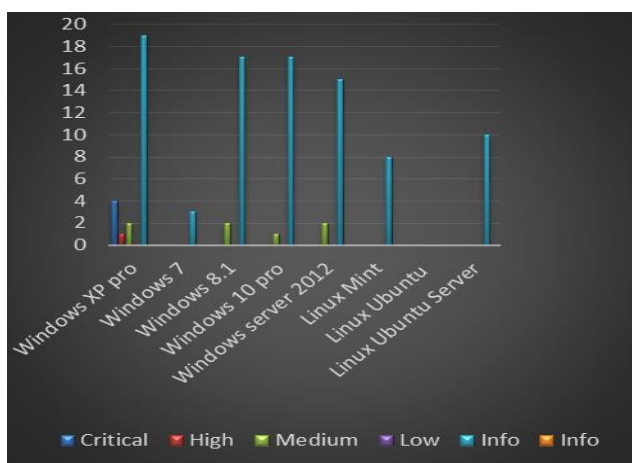


Figure 4. Classification of OSs Vulnerability by Severity (Nessus)

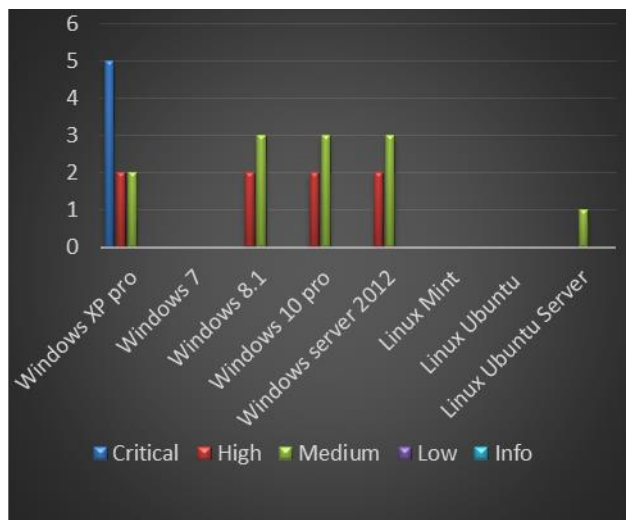


Figure 5. Classification of OSs Vulnerability by Severity (Retina)

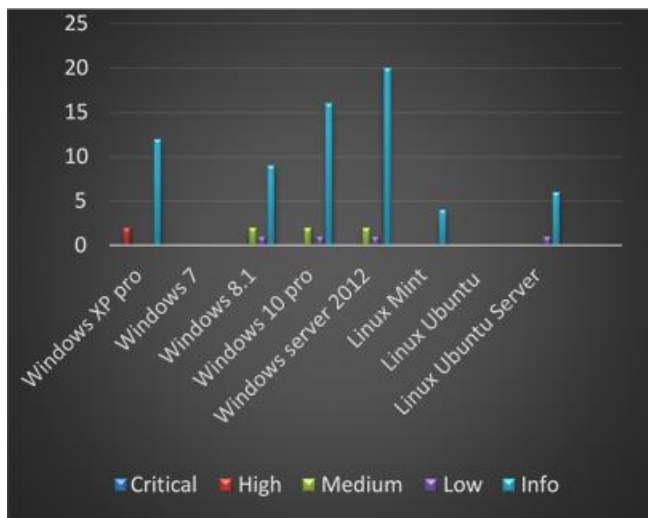


Figure 6. Classification of OSs Vulnerability by Severity (Nexpose)

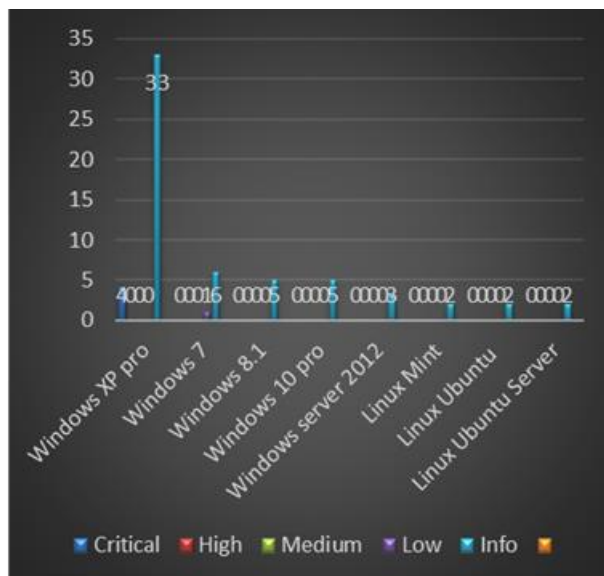


Figure 0. Classification of OSs Vulnerability by Severity (OpenVAS)

Regarding popular operating system that we have chosen as a test environment in our experimental setup, and according to the result found that windows 7 is the most secure and safe operating system among Microsoft products, less number of vulnerability discovered by the most powerful scanning tool, 10 vulnerability exciting in windows 7, followed by windows 8.1 which has 41 vulnerability, while windows 10 pro comes on the third place by 47 vulnerability, as can be clearly seen in the figure 8.

The total number of vulnerabilities discovered in Linux operating systems, the comparison among Linux products is done, and from the results, the most safe and secure operating system is Linux Ubuntu, 2 vulnerabilities discovered in the system, followed by Linux Mint, then Ubuntu Server.

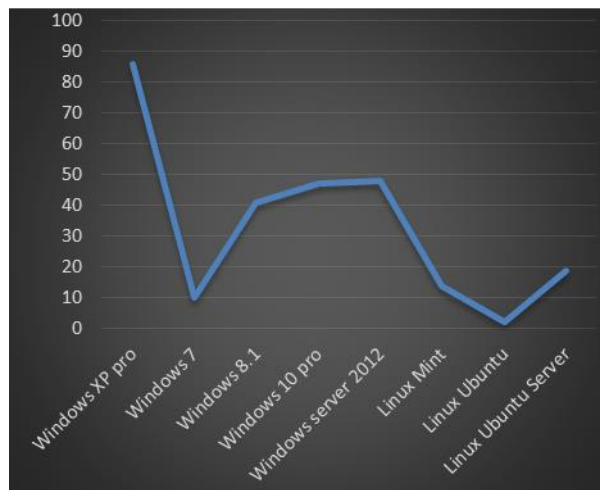


Figure 8. Popular Operating Systems Vulnerability

9. Recommendation

Generally, this paper relied on the practical method. We decided to give sufficient guideline through this work to the network administrators and go deeply inside experimental setup approach, providing full instruction, dealing with the modern techniques and tools used for accomplishing the task. Defense and mitigate attack strategy is to know the vulnerability and try to fix and patch them with the regular updating the software, check the application before installing the system, however, there are some application has malicious code, avoiding open any link or file has come from junk email, its recommended to use Gmail or Hotmail instead of yahoo mail, because Gmail almost filter all junk emails and files, use encryption when you deal with important action, and use site https (port 430) instead of site HTTP (port 80), A firewall and intrusion detection and prevention, antiviruses, sensors may not be useful and could not prevent cyber-attack if the database of them is not updated with new vulnerability.

10. Conclusion

With the highlights on comparing vulnerabilities of popular operating systems using well known vulnerability and penetration

testing tools moreover gives a sufficient guideline through this work to the users and go deeply inside experimental setup approach and provide instruction and dealing with the modern techniques and tools used for accomplishing the task. However, In the end penetration testing is the most approach of security process, by applying this approach can make your system more safely, rely on kind of security tool make your system in real danger, antiviruses and firewall are not enough to keep your system more secure, with the sophisticated tools and techniques of hackers can bypass the system. So, keeping the system automatically updated with the help security enhancement tools, as well as regular penetration testing, and vulnerability scanning can mitigate potential risks and threats.

References

- [1]Jimenez, W. Mammar, A. and Cavalli, A. "Software Vulnerabilities, Prevention and Detection Methods: A Review1," Security in Model-Driven Architecture, p. 6, 2009.
- [2]Steel C. and Nagappan, R. Core Security Patterns: Best Practices and Strategies for J2EE", Web Services, and Identity Management: Pearson Education India, 2006.
- [3]Vinod Varma Vegesna (2022). "Utilising VAPT Technologies (Vulnerability Assessment & Penetration Testing) as a Method for Actively Preventing Cyberattacks," International Journal of Management, Technology and Engineering, Volume XII, Issue VII, July 2022, Pages 81 94.
- [4]S. Raza and F. Jaison, "A Comparative Study between Vulnerability Assessment and Penetration Testing," Digital Forensics (4n6) Journal, May 2021
- [5]Allen, L. Heriyanto, T. and Ali, S. Kali Linux–Assuring Security by Penetration Testing: Packt Publishing Ltd, 2014.
- [6]Denis, M., Zena, C., &Hayajneh, T. (2016, April). Penetration testing: Concepts, attack methods, and defense strategies. In Long Island Systems, Applications and Technology Conference (LISAT), 2016 IEEE (pp. 1-6). IEEE.

- [7] Holik, F., Horalek J., Marik, O., Neradova, S. and Zitta, S. "Effective penetration testing with Metasploit framework and methodologies," in Computational Intelligence and Informatics (CINTI), 2014 IEEE 15th International Symposium on, 2014, pp. 237-242.
- [8] Holik, F., Horalek, J., Marik, O., Neradova, S., & Zitta, S. (2014, November). Effective penetration testing with Metasploit framework and methodologies. In Computational Intelligence and Informatics (CINTI), 2014 IEEE 15th International Symposium on (pp. 237-242). IEEE.
- [9] Holm, H. "Performance of automated network vulnerability scanning at remediating security issues," Computers & Security, vol. 31, pp. 164-175, 2012.
- [10] Juneja, G. K. "Ethical Hacking: A Technique To Enhance Information Security," International Journal of Innovative Research in Science, Engineering and Technology vol. 2, 2013.